IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

AMERICAN HOSPITAL ASSOCIATION, et al.,	§	
Plaintiffs,	§	
v.	§	Case No. 4:23-cv-1110-P
BECERRA, et al.,	§	
Defendants.	§	

BRIEF OF PATIENT JANE DOE AMICUS CURIAE IN OPPOSITION TO PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

Jason "Jay" Barnes*
Justin Presnal (TX00788220)
SIMMONS HANLY CONROY LLP
1 Court Street
Alton, IL 62002
(618) 259-2222
(618) 259-2220 (fax)
jaybarnes@simmonsfirm.com
jpresnal@simmonsfirm.com
**Pro hac vice forthcoming*

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

Rules

INTEREST OF AMICUS CURIAE

Jane Doe is a patient (hereinafter "Patient Amicus") putative class representative proceeding pseudonymously in a class action regarding the use of surveillance tools on healthcare provider websites.[1] Patient Amicus' interest in this litigation stems from her desire to protect her medical information, and that of others similarly situated, from unlawful and unauthorized surveillance, tracking, and disclosure. Patient Amicus respectfully submits this brief to provide the Court with relevant factual and legal information that Plaintiffs American Hospital Association, Texas Hospital Association, Texas Health Resources, and United Regional Health Care System (collectively "AHA") have ignored or misrepresented in their briefing.

Counsel for Patient Amicus represent hundreds of thousands of patients across the U.S. who have filed complaints against AHA members, including many Hospitals Amici. Those cases were filed as early as 2019—almost three years prior to the December 2022 HHS Bulletin, later clarified in March 2024 (together, the "Bulletin").[2] While liability in those cases is not predicated on HIPAA, HIPAA provides a guidepost for establishing a minimum standard of care and reasonable expectations of privacy. In addition, many states have codified HIPAA's Privacy Rule into state law. Thus, courts have scrutinized HIPAA's application to both authenticated and unauthenticated webpages. *See* Appx. A. At present, to counsels' knowledge, twenty-five out of twenty-five courts have denied motions to dismiss the entirety of any complaint. Critically, AHA cites one of those cases, *Kurowski v. Rush*, where the court initially held that "the interpretation of

[1] No party or counsel for a party authored this brief, in whole or in part, or made monetary contribution to fund the preparation or submission of this brief. No person other than amicus curiae and her counsel made a monetary contribution to its preparation or submission. All parties have consented in writing to the filing of this brief.

[2] Attached as Appendix A is a list of known cases, selection of illustrative complaints, and motion to dismiss rulings.

IIHI offered by HHS in its guidance goes well beyond the meaning of what the statute can bear." 2023 WL 4707184, at *4 (N.D. Ill. Jul. 24, 2023) (cited by the AHA Mot. at 21). But this was not, as represented by AHA, the final word by the *Kurowski* Court. Upon re-pleading, the *Kurowski* Court found additional allegations regarding disclosures of the name and location of a patient's personal physician and specialty (which occur on "unauthenticated" pages) sufficiently invoked HIPAA. *See* 2023 WL 8544084, at *2-3 (N.D. Ill. Dec. 11, 2023); *see also Cousin v. Sharp Healthcare*, 2023 WL 8007350, at *2-5 (S.D. Cal. Nov. 17, 2023) (disclosures of doctors, symptoms, treatments, and procedures on "unauthenticated" pages violated HIPAA and the California Medical Information Act, a state-based analog to HIPAA); *In re Group Health Plan Litig.*, 2023 WL 8850243, at *2 (D. Minn. Dec. 21, 2023) (same with respect to Minnesota's state-based analog to HIPAA).[3]

Indeed, patients' success in these litigations extends beyond the motion to dismiss phase to class certification. *See, e.g.*, *Doe v. Virginia Mason Med. Ctr.*, 2020 WL 1983046 (Sup. Ct. King County, Wash. Feb. 12, 2020) (certifying class of patients against Virginia Mason Medical Center for claims of invasion of privacy, identity theft, fraudulent concealment, unfair business practices, breach of the duty of confidentiality, and violation of the Washington Health Care Information Act (a state-analog to HIPAA)).

Against this backdrop, AHA, on behalf of its member hospitals, including Hospitals Amici, seeks to undermine the rulings in these other cases. AHA baselessly challenges the HHS Bulletin by moving for summary judgment on a factually deficient record through blatant forum shopping with a complaint and brief that omits key evidence. Simply put, these hospitals were unable to

[3] In *Rush*, *Cousin*, and *In re Group Health Plan Litig.*, defendant hospitals are all represented by the same counsel, Baker Hostetler, which is also the same firm that represents the Amici Hospitals.

defend against patients' claims on the merits in their own jurisdictions, so AHA and Hospitals Amici constructed this lawsuit to attempt to obtain a favorable ruling without the benefit of a full factual record. Patient Amicus provides factual background now.

INTRODUCTION

Patient Amicus files this brief in support of patient privacy rights that AHA and its members have subjugated to their own financial interests. The tracking technologies at issue in this lawsuit are not HIPAA-compliant analytical tools governed by Business Associate Agreements ("BAA") and regulations. Rather, the challenged tracking technologies are, in truth, arms of marketing giants like Facebook and Google and hundreds of other marketing surveillance companies financially motivated to exploit – not protect – patient privacy, without constraint or oversight. Notably, AHA and Hospitals Amici only address Google Analytics, even though they pervasively used tracking technologies that serve no function outside of targeted advertising.

The use of these technologies implicates privacy rights that have been codified in state and federal statutes for decades,[4] recognized at common-law,[5] and memorialized in the patient privacy policies of many Hospitals Amici.[6] In other words, HHS's Bulletin simply restates what HIPAA has explicitly prohibited for at least twenty years—hospitals cannot barter their patients' information for advertising benefits *without consent*. *See* 45 C.F.R. § 164.508(a)(ii)(3) (enacted

---

[4] *See e.g.,* Tex. Medical Records Privacy Act, Tex. Health & Safety Code Ann. § 181.152.

[5] *See Cloud v. Bert Bell/Pete Rozelle NFL Player Ret. Plan,* 2022 WL 1203099, at *1 (N.D. Tex. Apr. 21, 2022) (and collected cases) (recognizing a substantial privacy interest in medical information).

[6] *See, e.g.,* Hoag Memorial Hospital Presbyterian, "Patient Information," https://upload.cdn-hoag.org/wp-content/uploads/2022/11/04161032/10957_PatientInfoBooklet_1022_4b.pdf. (promising not to use or disclose patient information "for marketing purposes" or make "disclosures that constitute the sale of your medical information" without patients' written authorization); Torrance Memorial, "Notice of Privacy Practices," https://www.tmphysiciannetwork.org/app/files/public/8fa720fb-71e9-47b9-aa4a-68bc32931845/Torrance%20Memorial%20Physician%20Network/Pt%20Privacy/Notice-of-Privacy-Practices-TMPN.pdf ("We will not use or disclose your Health Information for marketing purposes without your written authorization."); SSM Health, "Notice of Privacy Practices," https://www.ssmhealth.com/privacy-notices-terms-of-use/notice-privacy-practices ("We are committed to protecting medical information about you" and do not make "disclosures of medical information for marketing purposes" without a patient's "written permission.").

2002) (using patients' health information for "marketing" requires express written consent); 45 C.F.R. § 164.514(b)(2)(i)(N) & (O) (enacted 2000) (prohibiting disclosure of patients' "Internet Protocol (IP) address numbers" and "Web Universal Resource Locators (URLs)" to third parties).

AHA moves for summary judgment on whether an individual's IP address, coupled with a "visit to an Unauthenticated Public Webpage that addresses specific health conditions or healthcare providers" (the "Proscribed Combination") constitutes IIHI. AHA Mot. at 11. As a threshold matter, *none of the tracking technologies at issue ever send IP addresses and URLs in isolation*. Rather, these tools also share user-agent information, device identifiers, and cookie values (including those linked to individual account holders) in conjunction with the Proscribed Combination. Thus, AHA seeks an "opinion advising what the law would be upon a hypothetical state of facts," which fails to satisfy Article III's case or controversy requirement. *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007).

AHA's motion also falls short on the merits. AHA argues an IP address "can never" be used to identify an individual and therefore falls outside the definition of IIHI. There is no evidence to support this statement. Indeed, it is patently untrue. AHA further argues the Proscribed Combination cannot be IIHI because hypothetical nonpatients may visit a hospital's web-property for reasons unrelated to healthcare. Neither the Bulletin nor HIPAA applies to information about nonpatients that is unrelated to their past, present, or future health care. The March 2024 clarification to the Bulletin explicitly states as much. Rather, AHA appears to invoke a bait-and-switch. That is, AHA requests a declaration that would invalidate the Bulletin to *both* patients and nonpatients. The Court should reject AHA's sleight-of-hand.

The Court should decline to hold, as a matter of law, that healthcare providers are free to barter their patients' health information to third parties without patient consent.

ARGUMENT

Summary judgment is only appropriate where the moving party "shows that there is no genuine dispute as to any material fact" and "is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). AHA fails to meet this burden.

AHA argues the Proscribed Combination (IP address and URLs of unauthenticated webpages) does not constitute IIHI as a matter of law because it "can never provide a reasonable basis to identify" an individual. ECF No. 25 ("AHA Mot.") at 25. Similarly, Hospitals Amici claim the tracking technologies do not "actually track the specific activities of individual users in a way that could ever be used to embarrass or otherwise harm them or subject them to potential criminal or civil exposure." ECF No. 35 ("Hosp. Am. Br.") at 11. But both claims are devoid of any factual support and thus insufficient to support, let alone permit AHA to succeed, on a motion for summary judgment. *See Ragas v. Tennessee Gas Pipeline Co.*, 136 F.3d 455, 458 (5th Cir. 1998) (noting "unsubstantiated assertions are not competent summary judgment evidence").

As set forth below, AHA's narrowly defined Proscribed Combination and Hospital Amici's characterization of tracking technologies are factually inaccurate. To start, the tracking technologies at issue transmit multiple identifiers bundled together—not just an IP address—in connection with patients' actions and communications. Moreover, this information is disclosed to some of the largest data companies in the world, including Facebook and Google. That is, these healthcare providers are providing this patient information to data companies who not only have long histories of broken privacy promises but are also most capable of misusing the disclosed information. Further, the transmissions are not one-off instances; they are successive transmissions of each and every action and communication that a patient makes on the healthcare provider's property. The net result is that hospitals are disclosing to third parties the full narrative of what a

patient is doing on their healthcare provider's property, culminating in a complete picture of the patient's actions and communications, including actions and communications on "unauthenticated" webpages and on "authenticated" pages. This factual clarification is important because the activity that AHA is challenging—which is *only* the Proscribed Combination—does not exist in the real world and does not account for the actual nature and volume of information being transmitted. AHA's challenge therefore has no practical effect because it is not addressing what is actually occurring.

I. HOW TRACKING TECHNOLOGIES ACTUALLY WORK

Many hospitals encourage patients to visit their web-properties to search for treatments, book appointments, contact providers, and access medical records through "patient portals." Unbeknownst to patients, many hospitals also embed their properties with tracking technologies from Facebook, Google, and other third-party marketing companies. These trackers share patients' information and online health activity with third parties, in real time, without patients' knowledge or consent.

To help the Court understand the full scope and scale of these tracking technologies, Patient Amicus' expert, Dr. Timothy Libert, analyzed forensic evidence of the Hospitals Amici's web-properties.[7] For the Court's convenience, summaries of the forensic evidence are available in a database at amicus.hospitalprivacy.org/about, which permits the Court to view the tracking technologies utilized by Hospitals Amici to third party marketing companies, including pages on which they appear. Critically, the database demonstrates that the transmissions to third parties go far beyond Google Analytics and far beyond disclosures for "analytical" purposes. For example, Alphabet as a whole—which includes various Google advertising arms like Google Ads and

[7] Prior to starting his own consulting practice, Dr. Libert was a privacy engineer at Google.

Google Display Ads—is present on 100% of the Hospital Amici websites; Oracle, a multinational data broker, is present on 20%; Rubicon Project, one of the largest online advertising companies, is present on 10%; and, The Trade Desk, an advertising platform that touts its ability to identify individuals across the open internet, is on 10% of the Hospital Amici websites.[8] Thus, the scope of the misconduct at issue is not cabined to just Google Analytics, nor limited to the purportedly benign ability to obtain aggregate user metrics and analytics, as AHA and Hospitals Amici would have this Court believe. The truth is far more nefarious—these entities are engaged in unauthorized disclosure of patient health information to third parties, the vast majority of whom are engaged in data mining, brokering, and online advertising.[9] As will be discussed below, the ability of these third parties to take the information disclosed about patients and use it to identify individuals is a critical consideration in whether information constitutes IIHI. This point that is blatantly ignored by AHA and Hospitals Amici.

To help the Court understand the tracking technology at issue, take the following example of a transmission that occurred on an "unauthenticated" webpage as a result of tracking technologies on Mercy Health's website (one of the Hospitals Amici). When a patient of Mercy visited https://www.mercy.com/health-care-services/primary-care-family-medicine/conditions/alcoholism, Mercy shared the URL with Google, along with the patient's: (1) IP address, (2) user-agent and information about her device properties, (3) cookies for Google, *and* (4) other persistent and unique cookies that operate as device identifiers. *This information is*

[8] https://amicus.hospitalprivacy.org/top_recipients. Notably, these percentages reflect the use of tracking technologies *after* the December 2022 Bulletin. These numbers would have been even higher before the Bulletin.

[9] Additional entities to whom Hospitals Amici disclose information include large marketing and data mining companies like: PubMatic, Salesforce, and Index Exchange. *See* https://amicus.hospitalprivacy.org/top_recipients.

more identifiable in the hands of companies like Facebook and Google than a name and home address. This occurred across Mercy's web properties, including communications related to appointment requests, specific doctors, specific treatments, and portal log-in and log-out pages. This is because Mercy placed the tracking technology on *every page* of its web property, thus ensuring that every patient action and communication was tracked, collected, and disclosed to third parties. By placing the tracking technologies on the patient portal log-in and log-out actions, Mercy disclosed the patient-status of individual patients to third parties, like Google, along with all previous communications about doctors, conditions, and treatments.

Thus, tracking technologies operate to transmit far more than just an IP address in connection with an "unauthenticated webpage." They also transmit numerous other identifiers, including those that are directly linked to consumer accounts, like Facebook and Google, along with actions taken, and content URLs that describe the precise medical condition that a patient is exchanging a communication about with their healthcare provider.[10] Further, tracking technologies occur on *every page*, thus providing third parties with a successive *history* of the patients' actions, including subsequent navigation to doctors' pages, appointment requests, patient portal actions, etc.[11]

AHA states that its complaint does not pertain to any "unauthenticated" webpage "that [either] require [or] request visitors to enter login information for user authentication." AHA Mot.

---

[10] *See, e.g.* Todd Feathers, Simon Fondrie-Teitler, Angier Waller, Surya Mattu, *Facebook Is Receiving Sensitive Medical Information Hospital Websites*, The Markup (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[11] *See, e.g.*, Andrew Downing, Jull Holdren, *Banned Tracking Technology Use Among Medical Device, Pharmacy, and Hospital Webforms: A Cross-Sectional Study*, submitted to the Journal of Medical Internet Research (March 15, 2024) (researching the prevalence of third-party tracking technology that appears on "unauthenticated" medical webpages on which patients enter and submit contact details).

at 6. But this distinction effectively eliminates their complaint because, in the real world, hospitals typically embed the ability to log-in or authenticate patient engagement on practically every page by listing patient portal access in the global header or footer.

Thus, the relief that AHA seeks conflicts with reality.

II. PLAINTIFFS LACK ARTICLE III STANDING

AHA's motion only applies to the legality of "online technology that connects (1) an individual's IP address with (2) a visit to an Unauthenticated Public Webpage that addresses specific health conditions or healthcare providers." AHA Mot. at 11. But, as detailed above, this limited combination of information is a legal fiction imagined by the AHA and Amici as a vehicle to obtain a ruling on a purported factual record that has no basis in reality. The tracking technologies at issue never send IP addresses and URLs in isolation. AHA therefore seeks an "opinion advising what the law would be upon a hypothetical state of facts." *MedImmune, Inc.*, 549 U.S. at 127. In other words, AHA does not present a case or controversy and therefore fails to clear the hurdles of Article III standing.

Even if the Court were to entertain the hypothetical scenario of a disclosure that only involved the very narrowly defined Proscribed Combination, such ruling would have no practical effect—*i.e.* redress no alleged harm—because the tracking technologies are not so limited in the disclosures made to third parties. Thus, Article III standing remains lacking. *See Lujan v Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (holding "it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision'"). AHA and Hospitals Amici allege they are harmed by a deprivation of their ability to use analytical tools, like Google Analytics. *See, e.g.* AHA Mot. at 17; Hosp. Am. Br. at 11-15. But a ruling on the Proscribed Combination will not (and should not) have any consequence on whether Google Analytics is or is not appropriate. Here, again, the reality of how the technology works is at odds with how AHA

has structured its requested relief. Google Analytics results in the transmission of far more information than just the IP address and the URL.[12] By limiting its challenge, AHA's requested relief would have no impact on the application of the Bulletin to the vast majority of its members' uses of tracking technologies. Thus, a ruling in AHA's favor will not redress the harm alleged. The Court should expressly decline to rule on any issue related to (1) disclosures of patient information via tracking technologies to marketing companies, and (2) any disclosures that involve anything more than the "Proscribed Combination."

It bears noting that Hospitals Amici complain (without evidence) that the Bulletin would prevent them from using "valuable website analytical tools" without "the risk of governmental sanction and penalty." Hosp. Am. Br. at 15. This argument is false. Hospitals Amici and all entities who fall within the purview of HIPAA may use analytical tools that result in the disclosure of patient health information *if they obtain informed written consent and when they obtain valid business associate agreements from the third parties*. *See* 45 C.F.R. § 164.508; 45 C.F.R. § 164.308(b). In other words, hospitals can utilize analytical tools when they comply with the law—the issue here is they want this Court to deem it permissible to share patient information in secret.

III. AHA HAS NOT PROFFERED ANY EVIDENCE TO SHOW IP ADDRESSES CANNOT BE USED TO IDENTIFY INDIVIDUALS

With respect to whether IP addresses are identifiable, as discussed below, AHA makes a series of factually unsupported, and inaccurate, claims as to why IP addresses do not fall under HIPAA's definition of "individual identifying information."

HIPAA expressly prohibits healthcare providers from disclosing "individually identifying

[12] Not to mention the fact that the vast majority of third-party recipients are not limited to "analytics" companies, but in fact are largely data brokers, data mining, and data advertising companies. *See* § I *supra.*

information" ("IIHI"), which is defined as information that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

45 C.F.R. § 160.103. AHA has not proffered any evidence—let alone undisputed evidence—to establish IP addresses cannot be used to identify individuals.

A. AHA Has Not Demonstrated That IP Addresses Are Not Personally Identifiable on Their Own

AHA argues an IP address "is not even remotely 'information' that provides a reasonable basis to identify 'the individual' (if any) whose own health, healthcare, or payment for health care actually 'relates to' the visit." AHA Mot. at 3. This argument is factually unsupported and, in reality, false.

IP addresses are widely recognized as individual identifiers under both federal and state law. *See, e.g.*, HIPAA Deidentification Rule, 45 C.F.R. § 164.514(b)(2)(i)(O); Children's Online Privacy Protection Act, 15 U.S.C. § 6501(4)(A) and 16 C.F.R. § 312.2 (defining "personal information" to include IP address); U.S. Dept. of Commerce, National Institute of Standards and Technology, Special Publication 800-122 (April 2010) at 14, 2-2 (including IP address in list of "examples of information that may be considered PII"). Likewise, law enforcement routinely relies on IP addresses to identify and locate criminal defendants. *See e.g., U.S. v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007); *U.S. v. Kim*, 677 F. Supp. 2d 930, 939 (S.D. Tex. 2009); *U.S. v. Torres*, 2016 WL 4821223, at *7 (W.D. Tex. Sept. 9, 2016).

In fact, many third parties that the healthcare providers in this case are disclosing information to, *e.g.*, Facebook and Google, keep a record of *every IP address* associated with a Facebook or Google user's account logins, which shows the association of IP addresses to individuals' accounts, along with their name, phone number, browser identifiers (labeled as user-agent), and cookie information.[13]

Thus, the reality is that IP addresses are personally identifiable under HIPAA because they *can and are used* to identify individuals. And, as discussed above (*see* § I), in the case of the tracking technologies at-issue, they are also associated with information related to the past, present, or future physical or mental health or condition of an individual. *See* 45 C.F.R. § 160.103. AHA has not presented any evidence to the contrary.

B. AHA Has Not Demonstrated IP Addresses Are Not Personally Identifiable in the Hands of Third Parties

As noted above, IIHI is defined under HIPAA to be information "with respect to which there is a reasonable basis to believe the information *can be used* to identify the individual." *See* 45 C.F.R § 160.103 (emphasis added). Thus, a determination of what "can be used" to identify the individual requires an understanding of the capabilities of the receiving third party. *See* 45 C.F.R. § 164.514(b)(1) (requiring "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable …[to] determine[] that the risk is very small that the information could be used, *alone or in combination with other reasonably available information, by an anticipated recipient* to identify an individual who is a subject of the information; and … [d]ocuments the methods and results of the analysis that justify such determination") (emphasis added).

[13] The Court can see this for itself by using Facebook's "Download Your Information" and Google's "Takeout" tools, each of which show the IP address and user-agent that Facebook and Google, respectively, associated with a specific user's login activity.

Indeed, HIPAA expressly takes this into consideration, as it requires that healthcare providers anonymize or "de-identify" health information *before sharing it with third parties*. 45 C.F.R. § 164.514. Specifically, HIPAA requires healthcare providers to remove identifying information, including "(M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; … (R) And any other unique identifying number, characteristic, or code." 45 C.F.R. § 164.514(b)(2). This is precisely the kind of information that the patients in the underlying privacy lawsuits allege that the Hospitals Amici disclosed, and, by its plain wording, IP addresses fall within this definition. It is also the kind of information that AHA now disingenuously suggests was subject to "new rulemaking" by the HHS. This is not a "new" rule. 45 C.F.R. § 164.514 was last amended in 2013—almost ten years prior to the issuance of the Bulletin.

As it pertains to the instant motion, AHA has not presented any evidence that IP addresses cannot be used by third-party recipients, like Facebook and Google, to identify individuals. The reason is obvious: AHA has no idea what happens to patient information after it is sent to Facebook and Google. These companies refuse to sign BAAs with hospitals and their data systems are some of the most closely guarded corporate secrets in the world.

However, even publicly available information shows that information like IP addresses can be and is used to routinely identify individuals. For example, Google operates an advertising exchange called Google Real Time Biding (RTB) that shares identifiable information with hundreds of other companies for advertising purposes.[14] Likewise, Facebook was famously caught

[14] *See, e.g.* https://developers.google.com/authorized-buyers/rtb/start; *see also* Timothy Libert, *Privacy Implications of Health Information Seeking on the Web*, Communications of the ACM, vol. 58, No. 3 (March 2025) (referencing a 2012 study that found that the use of IP addresses, along with other identifiers commonly sent to third parties, enabled researchers to identify users 80% of the time).

sharing its users' data with thousands of other companies in the Cambridge Analytica scandal.[15] Other companies, like Oracle, The Trade Desk, and PubMatic are actively engaged in the business of aggregating, profiling, and identifying individuals for purposes of online advertising.[16] Their business models are predicated on being able to match individuals with data, including health data, so that they can send them targeted advertising across multiple platforms and devices.[17]

Hospitals Amici argue Google Analytics is an innocuous program that "anonymizes the IP address;" is "not intended to spy on users;" and "maintain[s] the anonymity of individual users." Hosp. Am. Br. at 11, 15. But these statements (made in the absence of evidence) are both false and misleading. It is true that Google Analytics offers a self-described "IP anonymization" tool; however, that tool *does not anonymize the information sent to Google Analytics* because, if it did, Google Analytics would not work the way Google advertises. Instead, IP "anonymization" only redacts the last octet (last eight digits) of a patient's IP address *after Google receives the IP address (in full)* but before it is stored in Google's systems.[18] In any event, even with "the last octet"

---

[15] Nicolas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, The New York Times (April4, 2018), available at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[16] *See* https://techhq.com/2022/08/oracle-facing-data-backlash-for-violating-the-privacy-of-billions/ (reporting on Oracle data harvesting and privacy violations regarding information of five billion people); https://www.thetradedesk.com/us (The Trade Desk is an "omnichannel advertising platform built for the open internet").

[17] Indeed, many of these companies are engaged in the creation of "identity graphs," which compile various identifiers from individuals to create a single unified view of a customer across their devices, products, and websites. *See, e.g.* https://www.thetradedesk.com/us/resource-desk/how-identity-graphs-are-built-the-present-and-the-future; *see also* Timothy Libert, *Privacy Implications of Health Information Seeking on the Web*, *supra* (discussing the risks of third-party tracking and noting that many recipient companies have "massive data collection infrastructure that is designed to avoid detection, as well as ignore, counter-act, or evade user attempts at limiting collection" and that in many of these companies, the business model "is devoted to selling personal information").

[18] https://support.google.com/analytics/answer/2763052?hl=en.

redacted, the hospital still sends Google enough information for Google to uniquely identify the patient, including device and account identifiers such as cookies and user-agent information. For example, Google identifies patients primarily through a unique cookie called "_ga". Hospitals share this unique and persistent identifier with Google for each patient regardless of whether the hospital has "anonymized" the IP address.[19]

Again, the information Google collects through Google Analytics is not done in isolation. Rather, the information is *always* sent in combination with other identifiable information, in a single network transmission. Upon receipt, Google connects this information to other information it has already collected. For example, the "Google Signals" program (utilized by many AHA member hospitals) connects Google Analytics data with a patient's Google Account.[20] In addition, now-public documents from other litigation against Google establish that Google links various identifiers, including the _ga cookie, from Google Analytics with device identifying cookies from Google DoubleClick. *See Doe I, et al. v. Google, LLC,* 3:23-cv-02431-VC, Dkt. 61-5 at 8 (N.D. Cal.) (attached as Exhibit 1) (Google presented evidence that it was preserving "tables [that] contain mapping between Google Analytics User ID (UID) or client ID (CID) and Biscotti").[21] In turn, additional publicly available information reveals that Google connects Biscotti with even more information. *See Doe, I, et al. v. Google, LLC,* 3:23-cv-02431-VC, Dkt. 61-8 at 2-6 (N.D. Cal.) (attached as Exhibit 2) (stating "Google commingles signed-in and signed-out information"

[19] The information remains identifiable even in the absence of the _ga/cid cookie because redacting the IP address leaves the majority of the IP address intact. When combined with user-agent and device properties, the remaining IP address information remains unique enough to identify a specific patient in violation of 45 C.F.R. § 164.514(b)(ii), which was promulgated in December 2000, *i.e.* information that "could be used alone or in combination with other information to identify an individual who is a subject of the information".

[20] https://support.google.com/analytics/answer/9445345?

[21] "Biscotti" is the internal name for the device-identifying cookie for Google Display Ads, *i.e.* www.doubleclick.net.

in "files that simultaneously store [Google Account], Biscotti, and Zwieback IDs[22] and associated information (e.g. age, ethnicity, race, precise [geo]-coordinates, credit card data … device ID[s]….gender, income, children, education, shipping address" and "other identifiers").

In short, AHA's implication that third-party recipients, *e.g*. Google and Facebook, cannot identify patients via IP addresses is false and wholly unsupported by evidence – and contrary to common understanding. These large data and marketing companies in fact do use this information to identify individuals. That is precisely why it is illegal under HIPAA for healthcare providers to share patients' IP Addresses without express written consent. It is also why AHA cannot provide any actual evidence to support its claims to the contrary.

IV. AHA CANNOT EXPLOIT THE FIRST AMENDMENT TO EVADE ITS HIPAA OBLIGATIONS

AHA's suggestions that the First Amendment permits hospitals to sell patients' health information to Facebook and Google without consent is absurd, and based on a misapplication of *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011). Contrary to AHA's contentions, HIPAA's long-standing privacy protections present no "serious constitutional doubts." *See Jennings v. Rodriguez*, 583 U.S. 281, 286 (2018). Consequently, AHA cannot misuse the canon of constitutional avoidance to leverage a purported First Amendment concern to avoid long-established HIPAA obligations. "That is not how the canon of constitutional avoidance works. Spotting a constitutional issue does not give a court the authority rewrite a statute as it pleases. Instead, the canon permits a court to choose between competing *plausible* interpretations of a statutory text" *Id.* at 298 (citations and quotations omitted).

With respect to *Sorrell*, the Supreme Court invalidated a Vermont statute that restricted the

[22] "Zwieback" is the internal name for the device-identifying cookie for Google Ads, *i.e.* www.Google.com.

use of confidential government data regarding doctors' prescribing histories for marketing purposes but allowed the same data to be used for other purposes. *Sorrell*, 564 U.S. at 559–60. While recognizing that doctors have a confidentiality interest in their prescribing histories, the Court found Vermont's law constituted impermissible "viewpoint discrimination" because it specifically targeted marketers, whose speech Vermont's government disagreed with. *Id.* at 565–66. Making clear that *Sorrell* did not broadly invalidate all laws against the disclosure of confidential information, the Court narrowly focused on the Vermont statute's problematic discrimination between disfavored marketing speakers and other, favored speakers. *Id.* at 564. (noting that "[t]he law on its face burdens disfavored speech by disfavored speakers"). In doing so, *Sorrell* explicitly pointed to HIPAA as an example of the kind of privacy law that *does not* raise First Amendment issues that troubled the Court in *Sorrell*. *Id.* at 573. The *Sorrell* Court explained:

> HIPAA does not target disfavored speakers, but broadly protects confidential medical information while "allowing the information's sale or disclosure in only a few narrow and well-justified circumstances."

Id. (citation omitted). Indeed, HIPAA is unlike the law at issue in *Sorrell* because it allows patients to consent to the disclosure of their information without any rules designed "to advance a preferred message." *Id.* at 574–75 (explaining that "private decision making can avoid governmental partiality and thus insulate privacy measures from First Amendment challenge").

Applying the *Central Hudson* "intermediate scrutiny" test for laws regulating commercial speech, which the Supreme Court applied in *Sorrell*,[23] demonstrates that HIPAA's longstanding

[23] AHA mistakenly states that *Sorrell* applied "strict scrutiny." AHA Mot. at 22. While noting that some "heightened" scrutiny was required, *Sorrell* in fact applied the "intermediate scrutiny" test from *Central Hudson*, finding that "the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied." *Sorrell*, 564 U.S. at 572; *see also Vugo, Inc. v. City of New York*, 931 F.3d 42, 49–50 (2d Cir. 2019) (finding that the *Central Hudson* test continues to apply to commercial speech after *Sorrell*).

rule against disclosure of IP addresses or other identifying codes together with information about the individual's medical condition and/or treatment does not raise any "serious constitutional doubts." *See Jennings, supra*. As an initial matter, *Central Hudson* allows government regulation of any speech that is related to unlawful activity. *See Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 564 (1980) (holding that a state must assert substantial interest to regulate speech that is "neither misleading nor related to unlawful activity"); *see also Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 71 (1983) (noting "[t]he State may also prohibit commercial speech related to illegal behavior"). Numerous courts have denied motions to dismiss claims that AHA member hospitals' use of online tracking technologies is unlawful, including under state and federal wiretapping laws. *See* Appx. A; *see also Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 191 (5th Cir. 2000) (holding that First Amendment does not prevent application of wiretapping laws to news media). But even assuming AHA's First Amendment challenge could make it past that first step, HIPAA's privacy protections are plainly constitutional because they are (1) designed to achieve a substantial governmental interest and (2) drawn in proportion to that interest. *Central Hudson*, 447 U.S. at 564.

First, AHA incorrectly states that so long as the information being shared concerns communications exchanged while using a public webpage, HIPAA "implicates no real privacy interest[.]" AHA Mot. at 22. But courts have held that patients have a reasonable expectation of privacy, consistent with the historical norms of the doctor-patient relationship, on both authenticated and unauthenticated webpages. *See, e.g.*, Appx. at 67, 80, 81; *see also Sorrell*, 564 U.S. at 572 (recognizing state interest in protecting medical privacy). Furthermore, while—for litigation purposes—AHA professes that IP addresses "cannot reasonably identify" individuals (AHA Mot. at 22), its member hospitals—for business purposes—are busy using all kinds of

online tracking technologies designed to collect IP addresses precisely because the companies collecting this information believe that they *can* use it to identify individuals. Facebook and Google have become the most profitable advertising companies on the planet by using this kind of information to identify individuals in order to serve them targeted advertisements, and their success belies AHA's glib assertion that it "cannot reasonably" be done.

Second, HIPAA is drawn in proportion to the government's interests because it only prohibits the use of online trackers that disclose protected health information, allowing hospitals who wish to enable analytics or other helpful technologies without compromising privacy so long as hospitals comply with consent requirements, or obtain business associate agreements. *See* 45 C.F.R. § 164.508; 45 C.F.R. § 164.308(b); *Sorrell*, 564 U.S. at 573 (distinguishing HIPAA from the poorly drawn law at issue in *Sorrell* because HIPAA allows disclosure of private information "in only a few narrow and well-justified circumstances"). The fact that "many vendors"—such as those whose business model depends on exploiting information about Internet usage to sell advertising—find it "onerous" to comply with HIPAA's requirements (AHA Mot. at 23) is far from being a reason to scrap HIPAA's privacy protections. Rather, this highlights the pressures threatening medical privacy—profit over privacy—in the Internet context and shows how vital HIPAA continues to be.

As the Supreme Court held in *Jennings*, "[s]potting a constitutional issue does not give a court [or a regulated entity] the authority to rewrite a statute as it pleases." *Jennings*, 583 U.S. at 289. In *Jennings*, the Supreme Court reversed the Court of Appeals' use of the canon of constitutional avoidance, finding that the canon had no application because "the meaning of the relevant statutory provisions is clear." *Id.* at 848. Similarly, here, HIPAA clearly prohibits, and has been consistently interpreted for at least a decade to protect against, disclosure of IP addresses or

other identifying codes paired with information about the corresponding individual's health condition or treatment. This Court should therefore reject AHA's First Amendment argument.

CONCLUSION

For all these reasons, Patient Amicus respectfully requests that the Court deny Plaintiffs' Motion for Summary Judgment.

Date: March 28, 2024

Respectfully submitted,

/s/ Justin Presnal

Justin Presnal (TX00788220)
Jason "Jay" Barnes
SIMMONS HANLY CONROY LLP
1 Court Street
Alton, IL 62002
(618) 259-2222
(618) 259-2220 (fax)
jaybarnes@simmonsfirm.com
jpresnal@simmonsfirm.com

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

On March 28, 2024, I filed the foregoing document with the clerk of court for the U.S. District Court, Northern District of Texas. I hereby certify that I have served the document on all counsel and/or pro se parties of record by a manner authorized by Federal Rules of Civil Procedure 5(b)(2).

/s/ Justin Presnal
Justin Presnal